Notice of Allowability	Application No.	Applicant(s)	
	09/333,829	KIVINEN ET AL.	
	Examiner	Art Unit	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an amendment filed May 16, 2005*.

2. ☒ The allowed claim(s) is/are *1-13,16,17,24-28 and 30-33; renumbered as 1-24*.

3. ☒ The drawings filed on *15 June 1999* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Matthew Bsmithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Ronald Fish on May 23, 2005.

The application has been amended as follows:

IN THE CLAIMS:

For claims 1-13, 16-17, 24-28 and 30-33, Please delete "Allowed" and insert "Previously presented".

A clean copy of the amended changes to the claims are attached for scanning.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew T. Caldwell can be reached on (571) 272-3868. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137

Clean Copy of Amended Claims

IN THE CLAIMS:

1. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said intermediate computer devices may perform a network address translation or a protocol conversion resulting in alteration of a packet propagating therethrough, the method comprising the steps of

- determining what network address translations or protocol conversions, if any, occur on packets transmitted in a data path between said first computer device and the said second computer device on packets transmitted between said first computer device and said second computer device,
- if it is found that network address translations or protocol conversions occur in said data path between said first computer device and said a second computer device, taking packets conforming to a first protocol and using said first computer device to encapsulate them into packets conforming to a second protocol, which said second protocol being capable of traversing network address translations and protocol conversions,
- transmitting said packets conforming to said second protocol from said first computer device to said second computer device; and
- decapsulating said transmitted packets conforming to said second protocol into packets conforming to said first protocol.

2. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 1, wherein the step of taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol comprises the substeps of

- taking packets conforming to the Internet Protocol,
- processing said packets according to the IPSEC protocol suite and

- encapsulating the processed packets into packets conforming to the User Datagram Protocol.

3. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 1, wherein the step of taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol comprises the substeps of

- taking packets conforming to the Internet Protocol,
- processing said packets according to the IPSEC protocol suite and
- encapsulating the processed packets into packets conforming to the Transmission Control Protocol.

4. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 1, further comprising the step of compensating for the network address translations on said second protocol in the packets that are transmitted from said first computer device to said second computer device.

5. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 4, wherein said step of compensating for said network address translations comprises a step of performing address translation based on the information obtained in the step of determining what network address translations, if any, occur on packets transmitted between said first computer device and said second computer device.

6. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 5, wherein said step of compensating for said network address translations further comprises a step of performing port number translation based on the information obtained in the step of determining what network address translations, if any, occur on packets transmitted between said first computer device and said second computer device.

7. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 1, additionally comprising the step of periodically transmitting keepalive packets between said first computer device and said second computer device to ensure that said network address translations, if any, occurring on packets transmitted between said first computer device and said second computer device stay the same.

8. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method for conditionally setting up a secure communication connection between a first computer device and a second computer device through a

packet-switched data transmission network including intermediate computer devices, where at least one of said computer devices performs a network address translation or a protocol conversion or both a protocol conversion and a network address translation, the method comprising the steps of

- finding out, whether or not said second computer device supports a communication method where:

it is determined what network address translations or and/or protocol conversions or both, if any, occur on packets transmitted between said first computer device and said second computer device,

if it is found that network address translations or protocol conversions occur on packets transmitted between said first computer device and said second computer device, packets are taken that conform to a first protocol and encapsulated into packets that conform to a second protocol, which second protocol is capable of traversing network address translations and/or protocol conversions,

said packets conforming to said second protocol are transmitted from said first computer device to said second computer device,

and said transmitted packets conforming to said second protocol are decapsulated into packets conforming to said first protocol,

- as a response to a finding indicating that the second computer device supports said communication method, setting up a secure communication connection between said first computer device and said second computer device in which communication connection said communication method is employed and

- as a response to a finding indicating that said second computer device does not support said communication method, disabling use of said communication method between said first and said second computer devices.

9. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method for tunnelling packets between a first computer device and a second computer device through a packet-switched data transmission network comprising

intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion, the method comprising the steps of

- establishing a bidirectional tunnelling mode between said first computer device and said second computer device by exchanging packets conforming to a secure communication protocol,

- determining if one or more network address translations and/or protocol conversions occur on packets travelling from said first computer to said second computer, and if so, taking packets conforming to a first protocol and encapsulating them at said first computer device into packets conforming to a second protocol, which second protocol is capable of traversing network address translations,

- transmitting said packets conforming to said second protocol from said first computer device to said second computer device,

- decapsulating said transmitted packets conforming to said second protocol into packets conforming to said first protocol at the second computer device,

- obtaining information about the address translations occurred on packets transmitted between said first computer device and said second computer device and

- using said obtained information to modify the established bidirectional tunneling mode between said first computer device and said second computer device.

10. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 9, wherein the step of obtaining information about the address translations occurred on packets transmitted between said first computer device and said second computer device comprises the substeps of

- transmitting a packet between said first computer device and said second computer device, said packet comprising a header part and a payload part, and

- comparing a network address transmitted in said payload part to a network address transmitted in said header part in order to find out what changes have occurred on said network address transmitted in said header part.

11. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 9, additionally comprising the step of periodically transmitting keepalive packets between said first computer device and said second

computer device to ensure that network address translations, if any, occurring on packets transmitted between said first computer device and said second computer device stay the same.

12. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 9, wherein the step of using said obtained information to modify the operation of the tunnelling of packets comprises the substep of introducing an address translation before the encapsulation of packets in order to compensate for the network address translations that occur on packets transmitted between said first computer device and said second computer device.

13. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 9, wherein the step of using said obtained information to modify the operation of the tunnelling of packets comprises the substep of introducing an address translation after the decapsulation of packets in order to compensate for the network address translations that occur on packets transmitted between said first computer device and said second computer device.

14. (CANCELLED)

15. (CANCELLED)

16. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network including intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion and where a security protocol exists comprising a key management connection, the method comprising the steps of

- a method for determining what network address translations, if any, occur on packets transmitted between said first computer device and said second computer device:

establishing a key management connection according to said security protocol between said first computer device and said second computer device,

composing an indicator packet with a header part and a payload part of which both comprise the network addresses of said first computer device and said second computer device as seen by the node composing said packet,

transmitting and receiving said indicator packet within said key management connection;

and comparing in the received indicator packet the addresses contained in said header part and said payload part, and

- using the information concerning the determined occurrences of network address translations for securely communicating packets between the said first computer device and said second computer device.

17. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method according to claim 16, wherein the security protocol determines a standard port number for a key management connection, and the method further comprises the step of comparing in the received indicator packet a source port number against said standard port number for a key management connection.

18. (CANCELLED)

19. (CANCELLED)

20. (CANCELLED)

21. (CANCELLED)

22. (CANCELLED)

23. (CANCELLED)

24. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said intermediate computer devices may perform a network address translation and/or a protocol conversion resulting in alteration of a packet propagating therethrough, the method comprising the steps of

- determining what network address translations or protocol conversions, if any, occur on packets transmitted in a data path between said first computer device and said second computer device on packets transmitted between said first computer device and said second computer device,

- if it is found that network address translations and/or protocol conversions occur in said data path between said first computer device and said a second computer device, taking packets conforming to a first protocol and using said first computer device to encapsulate them into packets conforming to a

second protocol, said second protocol being capable of traversing network address translations and protocol conversions,

- transmitting said packets conforming to said second protocol from said first computer device to said second computer device.

25. (~~ALLOWED~~ PREVIOUSLY PRESENTED) The method of claim 24 further comprising the step of determining if said second computer device supports a secure data communication protocol prior to performing said step of determining what, if any, network address translations and/or protocol conversions are occurring in communications between said first computer device and said second computer device.

26. (~~ALLOWED~~ PREVIOUSLY PRESENTED) The method of claim 24 wherein the step of determining what, if any, network address translations or protocol conversions are occurring in communications between said first computer device and said second computer device is accomplished by:

sending at least one IKE Phase 2 Quick Mode message packet from said first computer device to said second computer device including in its private payload section IP addresses for an initator and responder as seen by said first computer device, where one of said first and second computer devices is said initiator and the other of said first and second computer devices is said responder; and

receiving at least one IKE Phase 2 Quick Mode message packet from said second computer device which was sent by said first computer device and including in its private payload section IP addresses for said initator and said responder as seen by said second computer device; and

in said first computer device, comparing said IP addresses in said header(s) of said at least one IKE Phase 2 Quick Mode message packet(s) received from said second computer device to said IP addresses in said private payload section, and, if there is a difference, concluding that a network address translation or a protocol conversion or both have occurred on the data path between said first computer device and said second computer device.

27. (~~ALLOWED~~ PREVIOUSLY PRESENTED) The process of claim 26 further comprising the step of periodically transmitting keepalive packets from said first computer device to said second computer device if it is determined that NAT or protocol conversions or both are occurring with the interval between

said keepalive packets being set to insure that mappings of said NAT or protocol conversions or both stay the same.

28. (~~ALLOWED~~ PREVIOUSLY PRESENTED) The method of claim 24 wherein the step of determining what, if any, port translations are occurring in communications between said first computer device and said second computer device is accomplished by comparing the port number in a packet header for a packet of a protocol that can withstand port translations and which encapsulates an IKE protocol packet sent from said second computer device to said first computer device, and if said port number is not a port number associated with the IKE protocol, concluding that one or more port translations is occurring on a data path between said second computer device and said first computer device.

29. (CANCELLED)

30. (~~ALLOWED~~ PREVIOUSLY PRESENTED) A method for conditionally setting up a secure communication connection and communicating data between a first computer device and a second computer device through a packet-switched data transmission network including intermediate computer devices, where at least one of said computer devices performs a network address translation or a protocol conversion or both a protocol conversion and a network address translation, the method comprising the steps of:

carrying out a negotiation between said first and second computer devices to determine if said second computer device supports a secure communication protocol which is incompatible with network address translations or protocol conversions or both;

as a response to a finding indicating that the second computer device supports said secure communication protocol, setting up a secure communication connection between said first computer device and said second computer device in which communication connection said secure communication protocol is employed;

as a response to a finding indicating that said second computer device does not support said secure communication protocol, disabling use of said secure communication protocol between said first and said second computer devices,

if it is found that said second computer device supports said secure communication protocol, determining what network address translations or protocol conversions or both, if any, occur on packets transmitted between said first computer device and said second computer device,

if it is found that network address translations or protocol conversions occur on packets transmitted between said first computer device and said second computer device, taking packets that conform to said secure communication protocol and encapsulating them into packets that conform to a second protocol, which second protocol is capable of traversing network address translations or protocol conversions, or both without violating said second protocol,

if it is found that network address translations or protocol conversions occur on packets transmitted between said first computer device and said second computer device, periodically transmitting keepalive packets from said first computer device to said second computer device with the interval between said keepalive packets being set to insure that mappings of said NAT or protocol conversions or both stay the same;

transmitting said packets conforming to said second protocol from said first computer device to said second computer device.

31. (~~ALLOWED~~ PREVIOUSLY PRESENTED) The method of claim 30 wherein said secure communication protocol is the IPsec protocol, and said second protocol is either the TCP or UDP protocol.

32. (~~ALLOWED~~ PREVIOUSLY PRESENTED) The method of claim 30 wherein said step of determining if said second computer device supports a secure communication protocol includes the step of finding out whether said second computer supports the IPsec protocol, and wherein said step of determining what network address translations or protocol conversions or both, if any, occur on packets transmitted between said first computer device and said second computer device comprises the steps:

sending at least one IKE Phase 2 Quick Mode message packet from said first computer device to said second computer device including in its private payload section IP addresses for an initator and responder as seen by said first computer device, where one of said first and second computer devices is said initiator and the other of said first and second computer devices is said responder, and

receiving at least one IKE Phase 2 Quick Mode message packet from said second computer device which was sent by said first computer device and including in its private payload section IP addresses for said initator and said responder as seen by said second computer device; and

in said first computer device, comparing said IP addresses in said header(s) of said at least one IKE Phase 2 Quick Mode message packet(s) received from said second computer device to said IP addresses in said private payload section, and, if there is a difference, concluding that a network address translation or a protocol conversion or both have occurred on the data path between said first computer device and said second computer device.

33. (~~ALLOWED~~ PREVIOUSLY PRESENTED) The method of claim 30 wherein the step of determining what, if any, port translations are occurring in communications between said first computer device and said second computer device is accomplished by comparing the port number in a packet header for a packet of a protocol that can withstand port translations and which encapsulates an IKE protocol packet sent from said second computer device to said first computer device, and if said port number is not a port number associated with the IKE protocol, concluding that one or more port translations is occurring on a data path between said second computer device and said first computer device.